UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,734	01/30/2002	Yves Audebert	L741.02101	5700

7590 11/21/2006

STEVENS, DAVIS, MILLER & MOSHER, L.L.P.
Suite 850
1615 L Street, N.W.
Washington, DC 20036

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,734	AUDEBERT ET AL.	
	Examiner	Art Unit	
	Venkat Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

The Applicant's response to arguments filed on 10/10/2006 are not persuasive. As U.S Patent 5309516 to Takaragi et al.(hereinafter Takaragi) discloses the communicating of first and second identifiers from first and second tokens to produce an key see Col 2 Ln 25-30. Takaragi discloses the use of office numbers and random numbers to generate an group key see Fig. 7 item 104. The group key is generated by using identifiers(identification information) along with the master key associated with the identifiers in form of an hash, which is the so-called group key.

The tokens of the instant invention relate to the IC Card of Takaragi, where the IC card maintains an memory of identification numbers and master keys to be used in forming the group key see Fig. 7. And further, Takaragi discloses the workstation also maintaining the same and generating the group key. And further of an communication network being shared by both the IC Card and the workstation for communication of the enciphered messages.

The Applicant's arguments regarding the single entity generating of key is not persuasive. Takaragi invention is not limited to generation of key by an single entity, the key is generated by the workstation as well as IC Card. And the communication of the keys between the IC Card and the workstation is also disclosed by Takaragi see Col 8 Ln 25-34. And this key shared among the IC Card and workstation are stored at the

memory see Fig. 1 item 127. The keys are generated using the destination id, where the id is pertinent to the office and person the user is associated with, thus is unique to each user.

Takaragi goes on to mention the exchange of information relating to generation of keys see Fig. 1, in particular the identification information and master keys. The IC Cards which initially have no information stored on to it, after communicating the workstation it is able to gain knowledge of the identification number and keys used for generating the group keys by the generation program. The interface on the IC Card and the Workstation provide means for communication between each other. Takaragi's invention is not limited to one token/one workstation, the possibility of many tokens connecting to the many workstations is suggested by Fig. 10.

Takaragi's invention is related to generation of key through the use of identification numbers unique to the user see Fig. 4, whereby at least the presence of an random number ensures the uniqueness of the id. And when this identification number is combined with the master key also unique to the user to form an group key. The group key is used for enciphering the message in communication network. The token and the workstation each generate the group key, in order to encipher/decipher message(i.e. an symmetric encryption). And exchanging of information from a token to another token in the network is also suggested by the use of keys derived from the information embodied in one token for enciphering the messages.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

Claims 1-8, 21, 24 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,309,516 to Takaragi et al.(hereinafter Takaragi).

Regarding Claim 1, Takaragi discloses the a data processing device for generating a unique key where an device includes means for combining group key with unique identifier received from token see Col 3 Ln 3-33; token having data storage for storing the unique key see Col 8 Ln 41-50 & Fig. 1 item 104 and cryptographic means for using unique key see Fig. 1 item 106 & Fig. 7 item 702.

Regarding Claim 2, 7, Takaragi discloses the exclusive OR operator see Col 11 Ln 45-55.

Regarding Claim 3, Takaragi discloses performing an hash function of the identifier and the group key see Col 8 Ln 61-Col 9 Ln 7.

Regarding Claim 4, 6, Takaragi discloses the digesting of unique identifier before operation see Fig. 4 & Col 8 Ln 51-60.

Regarding Claim 5, Takaragi discloses the generating a group key see Col 11 Ln 45-55; receiving a unique identifier from the first token and performing a operation with group key and unique identifier see Col 3 Ln 3-33; storing the generated unique key see Fig. 1 item 104; repeating for second token see Col 4 Ln 11-17 & Col 10 Ln 6-19.

Regarding Claim 8, Takaragi discloses the first token having a first unique identifier, an unique key that is a function of identifier and group key see Col 3 Ln 3-33, cryptographic means see Fig. 7 item 702, a memory means see Fig. 7 item 104; a second token having second unique identifier, an unique key that is a function of identifier and group key see Col 3 Ln 3-33 & Col 5 Ln 24-57; communication means for exchanging data between tokens see Col 6 Ln 45-52; first token having a first operator for processing first unique key and second identifier to produce an first composite key see Col 8 Ln 25-40 & Fig. 10 item 1005; a second token having a second operator for processing second unique key and first identifier to produce second composite key see Col 8 Ln 25-40 & Fig. 10 item 1003; first and second composite keys being equal see Col 9 Ln 58-Col 10 Ln 19 & Col 6 Ln 53-57.

Regarding Claim 21, Takaragi discloses the cipher function used by IC cards using the same key for encryption and decryption(symmetric cryptographic algorithm) see Col 3 Ln 3-32.

Regarding Claim 24, Takaragi discloses the program storage device performing the method step recited in Claim 5 see Fig. 2 item 202 & Fig. 1 item 108-114.

Claim Rejections - 35 USC § 103

Claims 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,309,516 to Takaragi et al.(hereinafter Takaragi) in view of U.S. Patent 5,694,471 to Chen et al.(hereinafter Chen).

Regarding Claim 9, 10, Takaragi discloses the second identifier(destination indicator) being processed by an first logic operator see Col 8 Ln 41-65 & Fig. 10 item 1011, first identifier(destination indicator) being processed by an second operator see Col 8 Ln 41-65 & Fig. 10 item 1009, but does not disclose a message digest function for digesting as it is commonly known in the art. However, Chen discloses the digesting of user identifier using MD5 see Col 7 Ln 58-67. It would be obvious to one having ordinary skill in the art at the time of the invention to include message digest of identifier(MD5) in the invention of Takaragi in order to obtain an shortened identifier for storage and processing(XOR) purposes as taught in Chen 4-21.

Regarding Claim 11 and 12, Takaragi discloses the second/first identifiers(destination identifiers) being processed see Col 8 Ln 25- 60 and further XORing of keys see Col 11 Ln 45-55, but does not disclose the XORing of keys and digest. However, Chen discloses the XORing of keys(unique identifiers) and digest to produce an composite

key see Col 8 Ln 1-8 and storing of the result see Fig. 2 item 150 & Fig. 1 item 2. It would be obvious to one having ordinary skill in the art at the time of the invention to include the XORing of keys and digest in the invention of Takaragi in order to have a secure result for encryption as taught in Chen see Col 8 Ln 9-21.

Claims 13-20, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,309,516 to Takaragi et al.(hereinafter Takaragi) in view of U.S. Patent 5,694,471 to Chen et al.(hereinafter Chen). as applied to claim 12 above, and further in view of U.S. Patent 6,067,621 to Yu et al.(hereinafter Yu).

Regarding Claim 13 and 14, Takaragi discloses the first and second destination indicator having an random value see Fig. 4 item 405 & Col 7 Ln 52-53 and storing of random number see Col 10 Ln 35-38 to produce an cryptograms see Fig. 3 item 306, but does not disclose the use of composite key. However, Yu discloses the random number (see Col 7 Ln 12-20 & Col 8 Ln 1-9) and the composite key to produce an cryptograms see Fig. 6 item 620-630 & Fig. 2 item 200-210.It would be obvious to one having ordinary skill in the art at the time of the invention to include the random number and the composite key to produce an cryptograms in the invention of Takaragi in order to produce secure message communications as taught in Yu see Col 11 Ln 44-58.

Regarding Claim 15 and 16, Takaragi discloses the decipher of random number from the cryptogram and keys see Col 2 Ln 16-45(random number from the destination indicators) & Col 8 Ln 30-40.

Regarding Claim 17 -20, Takaragi does not discloses the comparing of random numbers and it being used for authentication. However, Yu discloses the comparing of random number and it being used for authentication see Fig. 7 item 730, 770 & Col 7 Ln 36-46 & Col 11 Ln 12-58 & Col 8 Ln 10-16. It would be obvious to one having ordinary skill in the art at the time of the invention to include the comparing of random number and it being used for authentication in the invention of Takaragi in order to produce authentication as taught in Yu Col 12 Ln 11- 25.

Regarding Claim 22, The Examiner advises the Applicant to consult the table for appropriate rejections.

Part as Recited in Claim 22	See Corresponding Claim(s)/Rejection
a) sending a first ...	Claim 8
b) sending a second ...	Claim 8 and 9-10
c) digesting said first identifier...	Claim 9,10
d) performing an exclusive OR...second security token...	Claim 11, 12
e) performing an exclusive OR...first security token...	Claim 11, 12

f) generating a first random number...	Claim 13, 14
g) generating a second random number...	Claim 13, 14
h) sending said first...	Claim 13, 14
i) sending said second...	Claim 13, 14
j) receiving and decrypting said first ...	Claim 15, 16
k) receiving and decrypting said second	Claim 15, 16
l)sending said first ...	Claim 15, 16
m) sending said second...	Claim 15, 16
n) receiving said first...	Claim 17-20
o) receiving said second...	Claim 17-20
p) authenticating said second ...	Claim 17-20
q)authenticating said first...	Claim 17-20

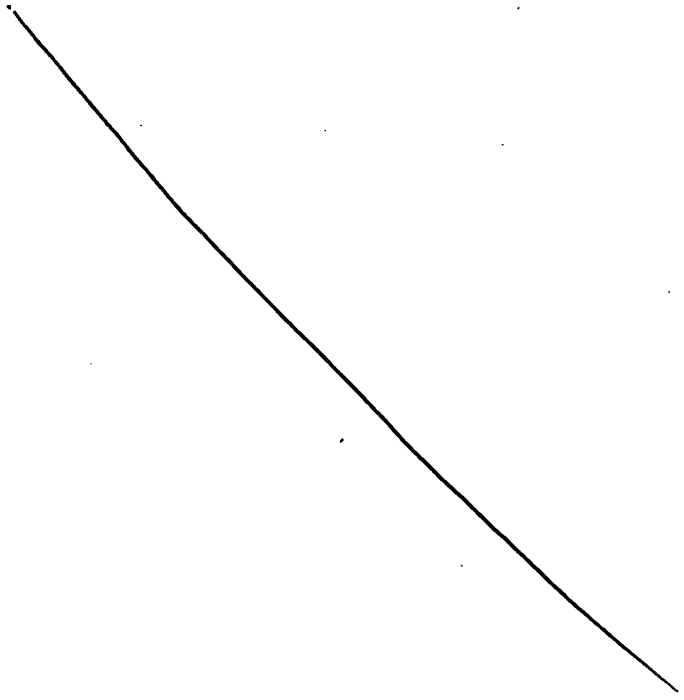
Regarding Claim 23, Takaragi discloses the cipher function used by IC cards using the same key for encryption and decryption(symmetric cryptographic algorithm) see Col 3 Ln 3-32.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action

and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Venkat Perungavoor
Examiner
Art Unit 2132

VP
11/16/06

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100